UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH, Plaintiff, v. TIKTOK, INC. et al., Defendants.	Case No. 5:23-cv-00964-SB-E ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS [DKT. NO. 24]

In this putative class action, Plaintiff Bernadine Griffith challenges Defendants TikTok, Inc. and ByteDance, Inc.'s use of software to collect information from non-TikTok users like Plaintiff when they visit third-party websites that have installed Defendants' software. Plaintiff alleges that Defendants' practices violate various privacy protections under federal and California law. Defendants move to dismiss Plaintiff's claims. Dkt. No. 24. The Court held a hearing on September 29, 2023, and now concludes that Plaintiff has adequately alleged all but her claims for violations of the Computer Fraud and Abuse Act and the Unfair Competition Law. The latter claims will be dismissed with leave to amend.

I.

The following facts are alleged in Plaintiff's complaint and taken as true for purposes of Defendants' motion to dismiss.

Defendants operate the social media application TikTok, which is used by more than 1 billion people worldwide (including 100 million in the United States)

to create, view, and share short videos. Dkt. No. 1 ¶ 2.[1] Defendants earn revenue through targeted advertising on the TikTok app, which depends on their use of users' data. *Id*. ¶ 19. Defendants have attracted significant negative attention for their privacy-related practices and have paid nearly a hundred million dollars to settle claims challenging their unauthorized collection of private data. *Id*. ¶ 3. Many U.S. residents, including Plaintiff, have chosen not to use TikTok because of their concerns about protecting their privacy. *Id*. ¶¶ 4, 74. However, Defendants have begun collecting data even from non-users of TikTok through the installation of Defendants' "TikTok SDK" software on third-party websites. *Id*. ¶ 5.

A software development kit, or SDK, is a package of prebuilt software tools that allows website developers to implement a particular function, such as billing or displaying advertisements. *Id*. ¶¶ 27–28. SDKs have become especially popular for online advertising, since they allow a website to connect to a larger advertising network that delivers personalized ads to users, collect user data to send to the ad network, and receive a share of the resulting ad revenue. *Id*. ¶ 29.

Advertising SDKs allow the delivery of personalized ads because they collect user data through "cookies"—small computer files that are automatically generated when a user visits a website. *Id*. ¶ 30. The cookie contains a string of text with information including the user's ID, email, or IP address. *Id*. Each time the user visits the website, the cookie on the user's hard drive is sent to the website for identification purposes. *Id*.

Defendants market their TikTok SDK as a tool to deliver more effective targeted advertisements, increasing ad revenue for the websites that install it. *Id*. ¶ 32.[2] When a user visits a website with the TikTok SDK installed, two cookies

---

[1] Defendants briefly assert in their motion that TikTok, Inc. is the entity that provides the TikTok platform to users in the United States, while ByteDance, Inc. is a separate entity. Dkt. No. 24 at 2 n.1. Defendants do not address Plaintiff's alter ego allegations, Dkt. No. 1 ¶¶ 10–12, or argue that they are inadequately pleaded. Accordingly, the Court, like the parties, does not distinguish between Defendants for purposes of this motion.

[2] To better understand the technology at issue in this case, the Court permitted each side to give a PowerPoint presentation at the September 8, 2023 scheduling conference. The parties' presentations used different terminology than the complaint at times; for example, Defendants asserted that their SDK involves advertisements to TikTok users and is not actually at issue here, and that the focus

are downloaded onto the user's hard drive: a "first-party" cookie that interacts with the website and a "third-party" cookie that Defendants can directly access. *Id*. ¶ 33. The cookies store a broad range of personal information, including email addresses, phone numbers, user IDs, browsing histories, and search queries. *Id*. A separate third-party cookie is downloaded from each website that has the TikTok SDK installed, which allows Defendants to monitor the user's activity across multiple websites. *Id*. ¶ 34. The third-party cookies allow Defendants to create detailed "digital dossiers" on individual users, including the user's unique ID number, IP address, browser, screen resolution, search terms, and a history of all websites visited that have the TikTok SDK installed. *Id*. ¶ 35.

The TikTok SDK also permits websites to use a "Pixel," which is a piece of JavaScript code that tracks user behavior by collecting (1) information about the ad a TikTok user clicked on or an event that was triggered; (2) the time the event was triggered; (3) the IP address of the user's computer, which indicates the user's geographic location; and (4) the make, model, and operating system of the user's device and the browser used to access the website. *Id*. ¶ 36. The Pixel also establishes third-party cookies by default and allows the website owner to implement first-party cookies. *Id*.

Web browsers typically have privacy settings that permit users to block third-party cookies. *Id*. ¶ 37. However, Plaintiff alleges that the TikTok SDK circumvents those settings by causing the websites to share first-party cookies with Defendants, "in effect transmuting a first-party cookie into a third-party cookie with the ability to evade web browser and operating system settings that would otherwise block it from reaching Defendants." *Id*. ¶ 38. Thus, Defendants are able to collect private data from users who have never used the TikTok app or registered for a TikTok account, who have no notice of TikTok's privacy policy or terms of use, and who have never consented to Defendants' collection of their data. *Id*. ¶ 39. Because the TikTok SDK is widely used by numerous websites, Defendants are able to aggregate data and assemble comprehensive profiles of non-TikTok users. *Id*. The combination of data facilitates digital "fingerprinting," which may allow Defendants to associate a profile with personally identifying information. *Id*. ¶¶ 41–42. Defendants use this information to improve their algorithms to predict users' interests. *Id*. ¶ 43.

---

of Plaintiff's allegations is really Defendants' "Pixel" code. For purposes of the Rule 12(b)(6) motion, however, the Court will only consider the complaint and any judicially noticed material.

User data has economic value, and a market for this data has emerged in the technology sector. *Id.* ¶¶ 44–45. The value of a single internet user's data is estimated to range from about $15 to more than $40. *Id.* ¶ 46. Although the value of data has largely been leveraged by corporations, it also may have economic value to the users themselves. *Id.* ¶ 50. Some companies and applications will now either pay internet users directly for their data or pay users to sign up and interact with the app. *Id.* Similarly, there is a private (and illegal) market for internet users' personal information, including Social Security numbers, banking information, and login credentials. *Id.* ¶¶ 53–54. Plaintiff therefore alleges that she and other class members have a quantifiable property right to their private data. *Id.* ¶¶ 55–58. She also alleges that class members who now understand Defendants' conduct must choose to either reduce their participation with the websites that use the TikTok SDK or accept less privacy than they were promised. *Id.* ¶ 61. Plaintiff further contends that she and other class members have suffered from the diminished value of their private data. *Id.* ¶¶ 65–67.

Plaintiff is a California resident who has never been a registered user of TikTok or held any TikTok account because she was concerned that TikTok would violate her privacy. *Id.* ¶ 74. She identifies three websites she frequently visited that installed the TikTok SDK, from which Defendants "secretly intercepted and collected her Private Data." *Id.* ¶ 75. Since 2017, Plaintiff has often used the Hulu video streaming service to watch television shows. *Id.* ¶ 76. Through the TikTok SDK, Defendants have obtained Plaintiff's data from Hulu, including information on the videos she searched for and watched. *Id.* Since June 2018, Plaintiff has been a member of the e-commerce website Etsy, from which Defendants have obtained information on what products she searched for, browsed, bought, and sold. *Id.* ¶ 77. Finally, in early 2022, Plaintiff visited the website of Build-a-Bear Workshop, which sells custom-built teddy bears. *Id.* ¶ 78. Because the website had the TikTok SDK installed, Defendants received information on the products she browsed and purchased. *Id.* Plaintiff alleges that these three websites are just representative examples of the hundreds or thousands of websites on which the TikTok SDK is installed. *Id.* ¶ 80.

Plaintiff alleges that she is "very conscious about her online privacy." *Id.* ¶ 79. She has changed the settings on her internet browsers to block third-party cookies and has enabled the "do not track" function. *Id.* She also uses security software to protect her online privacy. *Id.* However, the TikTok SDK circumvents these protective measures and obtains Plaintiff's private information by "transmuting its third-party cookie into a first-party cookie." *Id.*

In her complaint, Plaintiff alleges claims for (1) violation of the California Invasion of Privacy Act (CIPA), (2) violation of the federal Computer Fraud and Abuse Act (CFAA), (3) statutory larceny in violation of §§ 484 and 496 of the California Penal Code, (4) conversion, (5) violation of the California Unfair Competition Law (UCL), (6) invasion of privacy in violation of the California Constitution, and (7) intrusion upon seclusion. *Id*. ¶¶ 93–152. Plaintiff seeks to certify a nationwide class of non-TikTok users who have visited a website with the TikTok SDK installed, a similar nationwide class who also had settings to block third-party cookies, and subclasses consisting of the California residents within each class. *Id*. ¶ 82. Defendants move to dismiss Plaintiff's claims under Rule 12(b)(6) for failure to state a claim. Dkt. No. 24.[3]

II.

To survive a motion to dismiss under Rule 12(b)(6), a plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim has "facial plausibility" if the plaintiff pleads facts that "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In resolving a Rule 12(b)(6) motion, a court must accept all well-pleaded factual allegations as true, but "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," and courts "are not bound to accept as true a legal conclusion couched as a factual allegation." *Id*. (quoting *Twombly*, 550 U.S. at 555). Assuming the veracity of well-pleaded factual allegations, a court must "determine whether they plausibly

[3] Defendants also produce 11 exhibits that they assert are either incorporated by reference into the pleadings or subject to judicial notice. Dkt. No. 25. Plaintiff does not oppose Defendants' request for judicial notice and instead expands upon the request, providing additional materials that are related to Defendants' exhibits. Dkt. No. 36. Defendants have not objected to Plaintiff's materials. In the absence of a dispute, the Court declines to determine whether each of the proffered exhibits may be properly subject to judicial notice or considered under the incorporation by reference doctrine. *Cf. Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998–1003 (9th Cir. 2018) (describing both doctrines, their limitations, and the court's concern about their overuse). Most of the exhibits have no material impact on the Court's analysis. To the extent the Court relies on an exhibit, it has determined that the exhibit may be properly considered on Defendants' Rule 12(b)(6) motion.

give rise to an entitlement to relief." *Id.* at 679. There is no plausibility "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct." *Id.*

III.

A.

Defendants first challenge Plaintiff's claims in Counts 6 and 7 for invasion of privacy and intrusion on seclusion. Because of the similarity of these claims, courts consider them together, asking whether "(1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.* (*Facebook Tracking*), 956 F.3d 589, 601 (9th Cir. 2020) (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). Defendants focus only on the first inquiry, arguing that Plaintiff had no reasonable expectation that her communications with the three identified websites were private, both because of the nature of the information disclosed and because the websites notified Plaintiff that her activity may be forwarded to a third party.

Defendants rely heavily on several district court decisions addressing the existence of a reasonable expectation of privacy, but the Ninth Circuit's recent published decision in *Facebook Tracking* (which Defendants do not mention in their motion) is largely on point and provides the relevant legal standard. In that case, the plaintiffs challenged Facebook's practice of using cookies and embedded third-party plug-ins on third-party websites that captured user information after a user logged out of Facebook and visited other websites. Similar to the allegations here, the plaintiffs alleged that Facebook's tracking of its users allowed it "to amass a great degree of personalized information" including "an individual's likes, dislikes, interests, and habits over a significant amount of time, without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives." *Id.* at 599.

In assessing the viability of the plaintiff's claims for invasion of privacy under the California Constitution and for intrusion upon seclusion under California common law, the Ninth Circuit explained that "[t]he existence of a reasonable expectation of privacy, given the circumstances of each case, is a mixed question of law and fact." *Id.* at 601 (citing *Hill v. NCAA*, 7 Cal. 4th 1, 40 (1994)). To determine whether a reasonable expectation of privacy exists, courts "first consider whether a defendant gained 'unwanted access to data by electronic or other covert means, in violation of the law or social norms.'" *Id.* at 601–02 (quoting

Hernandez, 47 Cal. 4th at 286). This assessment requires courts to consider "a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities." *Id*. at 602. The Ninth Circuit in *Facebook Tracking* framed "the relevant question" as "whether a user would reasonably expect that Facebook would have access to the user's individual data after the user logged out of the application." *Id*.

The court held that the plaintiffs had plausibly alleged a reasonable expectation of privacy in the information Facebook collected, relying on both the fact that Facebook's disclosures might lead users to assume that only logged-in user data would be collected and on the amount and type of data collected. As to the latter, the court explained that "the amount of data allegedly collected was significant" because the plaintiffs alleged that Facebook acquired "an 'enormous amount of individualized data' through its use of cookies on the countless websites that incorporate Facebook plug-ins." *Id*. at 603 ("That this amount of information can be easily collected without user knowledge is similarly significant."). The court also found "[t]he nature of the allegedly collected data" to be important because Facebook obtained an individual's browsing history across various websites, which allowed it to acquire "an enormous amount of individualized data." *Id*. The court rejected Facebook's argument that the plaintiffs needed to identify specific sensitive information that Facebook collected, emphasizing instead that

> *both* the nature of collection and the sensitivity of the collected information are important. The question is not necessarily whether Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself. Rather, we must examine whether the data itself is sensitive *and* whether the manner it was collected—after users had logged out—violates social norms.

Id. Viewing the allegations in the light most favorable to the plaintiffs, the court concluded that "the allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits prevent us from concluding that the Plaintiffs have no reasonable expectation of privacy." *Id*. at 604.

At the pleading stage, Defendants have not demonstrated that *Facebook Tracking* is materially distinguishable. As in *Facebook Tracking*, Plaintiff alleges that Defendants have provided the TikTok SDK to numerous websites and use it to collect information about internet users' browsing activities that can be compiled

to "assemble a comprehensive profile of these non-TikTok users," all without the users' permission. Dkt. No. 1 ¶ 39. Plaintiff alleges that, simply from the three websites she has identified, TikTok collected information about the videos she searched for and watched, as well as products she browsed, bought, and sold on multiple websites. *Id*. ¶¶ 76–78.[4] These allegations do not appear to materially differ from the information allegedly collected in *Facebook Tracking*. And Defendants' argument that Plaintiff must more specifically identify sensitive data that Defendants collected from her was rejected in *Facebook Tracking*. 956 F.3d at 603 (rejecting argument "that Plaintiffs need to identify specific, sensitive information that Facebook collected, and that their more general allegation that Facebook acquired 'an enormous amount of individualized data' is insufficient").

To be sure, the court in *Facebook Tracking* emphasized that "Facebook's privacy disclosures . . . allegedly failed to acknowledge its tracking of logged-out users, suggesting that users' information would not be tracked," such that reasonable users would not expect to be tracked while not logged in. *Id*. at 602. But Defendants have not shown that their alleged tracking of non-users' activity is any less violative of social norms or expectations than Facebook's tracking of its users' activity while they were not logged into Facebook. It is plausible that an internet user who has avoided using TikTok because of privacy concerns might be just as alarmed to find that TikTok is collecting her browsing data as a Facebook user would be to discover that Facebook tracks her conduct when she is logged out. And to the extent Defendants argue that the nature and utility of the data collected in *Facebook Tracking* differs from that of the data collected by the TikTok SDK, no material differences are evident from the face of Plaintiff's pleading. Thus, viewing the allegations in the light most favorable to Plaintiff, she has plausibly

[4] In her opposition, Plaintiff also relies on allegations in her complaint about other personal information that can be collected by the TikTok SDK, including phone numbers and email addresses, as well as sensitive information such as searches for medical conditions, contraceptives, and addiction treatment facilities. *See* Dkt. No. 1 ¶¶ 5, 28, 33, 36. 40. But Plaintiff does not allege that TikTok obtained her phone number or email address or that she searched for any particularly sensitive information, so these allegations have little bearing on whether Plaintiff has stated a claim for violation of her privacy rights. *Cf.* *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 816 (N.D. Cal. 2020) (explaining that allegations about intercepted sensitive conversations did not establish named plaintiffs' reasonable expectation of privacy where the communications were not alleged to have been made by the named plaintiffs).

alleged that Defendants "gained unwanted access to [Plaintiff's] data by electronic or other covert means, in violation of the law or social norms," thereby violating Plaintiff's reasonable expectation of privacy. *Id*. at 601–02 (cleaned up); *accord* *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1089 (N.D. Cal. 2022) ("Plaintiffs have plausibly alleged a reasonable expectation of privacy because Google allegedly collected potentially sensitive data while users might not expect that Google was tracking them.").

Defendants' reliance on pre-*Facebook Tracking* cases to argue that there is a presumption that internet communications do not give rise to an expectation of privacy is unavailing. Defendants' principal authority, *People v. Nakai*, is a criminal case that made no mention of any presumption and merely held, on the facts of that case, that the defendant could not reasonably expect his chat to be private. 183 Cal. App. 4th 499, 518 (2010) (explaining that any expectation of privacy was unreasonable because (1) "the Yahoo! privacy policy indicated that chat dialogues may be shared for the purpose of investigating or preventing illegal activities," (2) "Yahoo! warns users that chat dialogues can be 'archive[d], print[ed], and save[d],'" (3) "defendant was communicating online with a person whom he did not know, via writing and photographs," and (4) "defendant expressed concern that dark_dana_666's mother would discover their communications, which reflects awareness that dark_dana_666's communications could be viewed or intercepted by her mother"). *Revitch v. New Moosejaw, LLC*, on which Defendants also rely, discussed a presumption of nonconfidentiality in the context of CIPA. 18-CV-06827, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019). In connection with the common law and constitutional privacy claims, however, the court in *Revitch* denied the defendants' motion to dismiss because their code allegedly allowed them to associate the plaintiff's browsing habit with his identity, "a highly offensive breach of norms." *Id*. The court also noted that "[u]nder California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *Id*. (quoting *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019)). Here, Plaintiff has similarly alleged that the TikTok SDK allows Defendants to assemble extensive profiles containing individuals' browsing histories across numerous websites, and, as in *Revitch*, the Court cannot conclude at the pleading stage that the alleged privacy intrusion is not serious.

Nor have Defendants shown that Plaintiff's claim necessarily fails because the websites' privacy policies disclosed that they would collect and share her data. Defendants clarified at the hearing that they are not at this stage asserting that Plaintiff's claims are barred under the doctrine of consent, but merely arguing that

Plaintiff's awareness that the websites would disclose some of her information to third parties is a factor tending to show that she lacked a reasonable expectation of privacy in her data. Defendants' argument rests not on Plaintiff's allegations but rather on privacy policy documents from the three websites Plaintiff identifies in the complaint, of which Defendants ask the Court to take judicial notice. The Court need not recite the details of the exhibits produced by the parties; it is undisputed that the privacy policies generally disclosed that some of Plaintiff's information would be shared with third parties but did not specifically provide that it would be given to TikTok (even when providing detailed lists of other third-parties whose cookies were present on the websites). There is no allegation that Plaintiff read any of these policies or that these policies reasonably disclosed the true scope and import of the third-party sharing. In any event, given Plaintiff's specific privacy concerns about TikTok, Defendants' size and ability to collect information from numerous websites, and the absence of any communication from TikTok that it was collecting her data, Defendants have not established that Plaintiff consented to TikTok's receipt of her information or that Plaintiff's claims must be dismissed at the pleading stage because she lacked a reasonable expectation of privacy. *Cf.* *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) (Koh, J.) ("If a reasonable user could have plausibly interpreted the contract language as not disclosing that the defendant would engage in particular conduct, then the defendant cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)." (cleaned up)).

B.

Defendants next argue that Plaintiff's CIPA claims in Count 1 fail as a matter of law. Plaintiff alleges violations of two provisions of CIPA: §§ 631(a) and 632(a) of the California Penal Code. The Court begins its analysis with the latter.

Section 632 imposes liability on "[a] person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication" of another. Cal. Penal Code § 632(a). Defendants raise two arguments for dismissal of Plaintiff's § 632 claim.

First, relying on their arguments already discussed above, Defendants argue that Plaintiff fails to allege that any "confidential communication" was recorded because CIPA's confidentiality standard requires the same analysis as the question of whether Plaintiff has a reasonable expectation of privacy. It is not clear as a

matter of law that the CIPA confidentiality analysis is identical in all respects to the reasonable expectation of privacy analysis; the authority Defendants cite for this proposition merely states that the analysis of the two issues in that case is "similar." *In re Meta Pixel Healthcare Litig.*, 22-CV-03580, 2022 WL 17869218, at *15 n.12 (N.D. Cal. Dec. 22, 2022). But even assuming the validity of Defendants' premise, their argument fails because, as discussed above, Plaintiff has adequately alleged a reasonable expectation of privacy under *Facebook Tracking*.

Second, Defendants argue that even if the TikTok SDK constitutes a "recording device," Plaintiff has not alleged that Defendants used it, because individual website owners make the decision to employ the code and determine what data to disclose when they configure it. The sole case on which they rely in their motion is *Lopez v. Apple, Inc.*, in which the court *rejected* Apple's argument that it did not use a recording device because the plaintiffs controlled their own phones. 519 F. Supp. 3d 672, 690 (N.D. Cal. 2021) ("Plaintiffs allege that Apple used the devices by programming Siri software to intercept communications when no hot word was spoken. This states a claim for eavesdropping because it involves 'secretly listening to a conversation between two other parties.' Apple cites no case to show that anything more is required." (citation omitted)).

More importantly, Defendants' Rule 12(b)(6) motion challenges the adequacy of Plaintiff's pleading, but their argument relies heavily on their assertions—not contained in the complaint—about how the TikTok SDK is implemented and the agency of the websites in deciding what data to collect. Plaintiff alleges that Defendants created the TikTok SDK to facilitate their collection of data, that they provide it to websites for that purpose, and that they receive data from the cookies the TikTok SDK places on website visitors' computers. It is not evident from the face of the complaint that the websites act in a vacuum, independent of Defendants' influence, as Defendants suggest. Indeed, Defendants ask the Court to take judicial notice of a document in which they "recommend" that websites use the code expansively and note that the third-party cookie is "on by default." *See* Dkt. No. 25-2 at 2 of 3 ("[W]e recommend you set up events that reflect a full customer journey of your site from viewing a product details page to adding an item to a cart and making a purchase."). Defendants identify no authority suggesting that they cannot be held liable for eavesdropping because a third party, acting on Defendants' recommendation, participated in the installation of Defendants' code that sends information to Defendants. Defendants also acknowledged at the hearing that a code developer could under some circumstances be liable for a third-party website's use of the code. At the pleading

stage, the Court is unable to resolve the parties' factual dispute about whether the websites' decisions break the causal chain from Defendants' acts such that Defendants are insulated from liability for their dissemination of the TikTok SDK and their collection of the data they receive from it. Accordingly, Defendants have not shown that Plaintiff's claim for violation of § 632 should be dismissed.[5]

Because Count 1 plausibly alleges a violation of CIPA based on § 632, it is unnecessary for the Court to decide at the pleading stage whether it also plausibly alleges an alternative basis for CIPA liability under § 631. Rule 12(b)(6) "does not provide a mechanism for dismissing only a portion of a claim." *Franklin v. Midwest Recovery Sys., LLC*, 8:18-CV-02085-JLS, 2020 WL 3213676, at *1 (C.D. Cal. Mar. 9, 2020) (collecting cases); *accord BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015) ("A motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of *parts* of claims; the question at this stage is simply whether the complaint includes factual allegations that state a plausible claim for relief."). Thus, the Court does not reach Defendants' arguments challenging § 631 liability. *See Doe v. Napa Valley Unified Sch. Dist.*, No. 17-CV-03753, 2018 WL 4859978, at *3 (N.D. Cal. Apr. 24, 2018) (denying motion to dismiss some theories of negligence for failure to state a claim where plaintiff had stated a cause of action under another theory).

C.

In Count 2, Plaintiff alleges that Defendants violated the CFAA by exceeding their authorized access to Plaintiff's and class members' computers. *See* 18 U.S.C. § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section."). The CFAA permits a private cause of action by a person who "suffers damage or loss" as a result of a CFAA violation, but only if the conduct involves one of the factors set forth in § 1030(c)(4)(A)(i)(I)–(V). *Id.* § 1030(g). Plaintiff invokes two of these factors, contending that Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . .

[5] The Court expresses no opinion as to the ultimate viability of Plaintiff's § 632 claim and does not intend to suggest that Defendants will be unable to prove that Plaintiff's claim fails because they lacked the requisite agency. It merely holds that Defendants' narrow arguments, supported by sparse legal authority, do not establish that they are entitled to dismissal at the pleading stage.

aggregating at least $5,000 in value" and "a threat to public health or safety." *Id.* § 1030(c)(4)(A)(i)(I), (IV). Defendants argue that Plaintiff's claim fails both because they did not access her computer and because she has not alleged the requisite harm.

Defendants cite authority describing the purpose of the CFAA to argue that they are not alleged to have engaged in any conduct akin to computer hacking. *E.g.*, *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022) ("The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking."). Defendants do not appear to dispute that the placement of cookies on Plaintiff's computer can constitute a violation of the CFAA. *See In re Toys R Us, Inc., Priv. Litig.*, No. 00-CV-2746, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001) (holding that allegation that defendants caused a cookie to be implanted in plaintiffs' computers stated a claim under the CFAA). Instead, they repeat their argument that it was the website owners, not Defendants, who placed the code on their websites. But Defendants cite no authority holding that someone who develops a code that is designed to surreptitiously place cookies on users' computers in violation of the CFAA and encourages others to implement the code for that purpose is absolved of liability when the cookies are installed and perform their intended function. Moreover, as explained above, Defendants' argument relies on disputed or undeveloped facts about the relative roles of Defendants and the website owners that cannot be accepted as true on a pleading challenge.

Defendants also argue that Plaintiff's CFAA claim fails because she has not alleged either cognizable harm aggregating at least $5,000 in value or a threat to public health or safety. As to the former, Plaintiff argues that she has alleged "out-of-pocket costs" resulting from Defendant's violations, including the purchase of security software, but she makes no argument that such costs exceed the $5,000 threshold. And while her complaint conclusorily alleges aggregate losses of at least $5,000, Dkt. No. 1 ¶ 108, it identifies no factual basis for this assertion.

Plaintiff focuses more heavily on her allegation that Defendants' conduct constitutes a threat to public health or safety. She relies on the complaint's recitation of President Trump's statement in a 2020 executive order that the use of TikTok in the United States "threatens to allow the Chinese Communist Party access to Americans' personal and propriety information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." *Id.* ¶ 22. She also selectively quotes from a single case, *Vaquero Energy, Inc. v. Herda*,

which found a threat to public health and safety based not only on access to personal and financial data (which Plaintiff notes) but also on the fact that the programs at issue controlled "extensive and critical oil and gas production facilities in close connection to residential and commercial areas" (which Plaintiff omits). 1:15-CV-0967, 2015 WL 5173535, at *8 (E.D. Cal. Sept. 3, 2015). Thus, alteration of the targeted computer program "could cause 'a H2S gas release, high pressure steam release, fire, oil spill, or pipeline rupture.'" *Id*.

Here, in contrast, Plaintiff has not alleged that the TikTok SDK's placement of cookies on her computer presents any threat to public health or safety. She does not allege that she is a federal employer or contractor, that the information gathered by TikTok may be used to blackmail her or commit corporate espionage, or that it threatens to cause physical or environmental harm. To the extent Plaintiff's argument is that the TikTok SDK threatens public safety when it collects the data of other class members who are federal employees or hold other sensitive positions, she does not identify any authority permitting her to state a claim based only on a threat that does not apply to her. Because she has not plausibly alleged that the intrusion on her computer caused the type of harm required for a private cause of action under § 1030(g), Plaintiff has not alleged a plausible claim for violation of the CFAA, and Count 2 is dismissed.

D.

Defendants argue that Plaintiff's claims for statutory larceny in Count 3 and conversion in Count 4 fail because Plaintiff has no property right in the data that Defendants acquired—undisputedly a requirement of both claims. Defendants rely principally on *Low v. LinkedIn Corp.*, in which Judge Koh dismissed a conversion claim based on the defendant's alleged disclosure of the plaintiffs' personal browsing history and other personally identifiable information because "the weight of authority holds that a plaintiff's 'personal information' does not constitute property." 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012). But in her more recent decision in *Calhoun*, Judge Koh rejected Google's reliance on *Low*, finding that—consistent with a "growing trend across courts"—the taking of personal information was adequate to allege deprivation of a property interest:

> Google ignores this Court's other rulings, both before and after *Low v. LinkedIn*. *See, e.g.*, *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 798–99 (N.D. Cal. 2011) (plaintiffs' names were misappropriated and thus lost value which constituted an injury to plaintiffs); *In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May

> 17, 2016) (plaintiffs' personal information was stolen in a data breach and thus lost value which constituted an injury to plaintiffs); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (same).
>
> Similarly, courts have recognized the "growing trend across courts . . . to recognize the lost property value" of personal information. *In re Marriott Int'l, Inc. Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) (concluding that personal information has value); *see also In re Facebook Privacy Litigation*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims).
>
> Furthermore, California courts have also acknowledged that users have a property interest in their personal information. *See CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860 (2006) ("A person's identifying information is a valuable asset."); *accord Facebook Tracking*, 956 F.3d at 600 (citing *Lepe* and holding that the plaintiffs had suffered economic injury after Facebook allegedly took their personal information in a similar process to that alleged here). Accordingly, Plaintiffs have adequately alleged that they were deprived of a property interest.

526 F. Supp. 3d at 635.

Defendants concede in their reply (which significantly expands on their one-paragraph argument in the motion) that personal information *can* be property, but they argue that Plaintiff's browsing history and search information is not property, in part because it belongs equally to the websites she visits. At the hearing, they focused on their assertion that the data they obtain from non-users is a valueless by-product that they only collect because they are unable to separate it from TikTok users' data (which is valuable to Defendants) on the front end. Plaintiff disputes this assertion, which in any event is outside—and contrary to—the pleadings.

Plaintiff's complaint contains several pages of allegations describing the value and marketability of internet user data, including the opportunities for internet users to directly sell or otherwise monetize information about their online

activity. Dkt. No. 1 ¶¶ 44–55. Viewing these allegations in the light most favorable to Plaintiff, and particularly given the evolving case law recognizing property interests in such information, Defendants have not shown as a matter of law that Plaintiff's allegation that she had a property right in the data Defendants collected is implausible.

E.

Finally, Defendants move to dismiss Plaintiff's UCL claim in Count 5. The UCL "requires that a plaintiff have 'lost money or property' to have standing to sue," which requires the plaintiff to "demonstrate some form of economic injury." *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011). This requirement was enacted "to confine standing to those actually injured by a defendant's business practices and to curtail the prior practice of filing suits on behalf of clients who have not used the defendant's product or service, viewed the defendant's advertising, or had any other business dealing with the defendant." *Id*. at 321 (cleaned up). The UCL's requirement of economic injury "renders standing under [the UCL] substantially narrower than federal standing under article III, section 2 of the United States Constitution, which may be predicated on a broader range of injuries." *Id*. at 324. Plaintiff asserts two types of economic injury: the loss of her private data and the diminution of its value. Defendants contend that neither is adequate.

The case law on this issue is not a model of clarity. Plaintiff relies on *Calhoun*, which states that "the Ninth Circuit and a number of district courts . . . have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing" under the UCL. 526 F. Supp. 3d at 636 (collecting cases). But the sole Ninth Circuit case cited for this proposition in *Calhoun* held the opposite: It found that allegations "that the information disclosed by Facebook can be used to obtain personal information about plaintiffs, and that they were harmed both by the dissemination of their personal information and by losing the sales value of that information" were sufficient to establish the damages elements of the plaintiffs' breach of contract and fraud claims, but *not* to establish UCL standing. *In re Facebook Priv. Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) ("We affirm the district court's dismissal of plaintiffs' UCL claim because plaintiffs failed to allege that they 'lost money or property as a result of the unfair competition.'"). The district court decision affirmed in that case held that "personal information does not constitute property for purposes of a UCL claim." *In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011). It distinguished authority permitting UCL claims by customers whose financial

information had been disclosed by an internet service provider, because unlike in that case, the plaintiffs had not paid for the defendant's services, so they were not consumers who had received less than the benefit of their bargain. *Id*. at 714–15 (distinguishing *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010)).

Other district courts addressing UCL standing have reached similar conclusions. *See, e.g.*, *Jackson v. Loews Hotels, Inc.*, No. ED-18-CV-827-DMG, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) ("Courts in this circuit have held that 'theft' or 'unauthorized release of personal information' does not qualify as lost money or property for purposes of determining standing under the UCL." (collecting cases)). However, some district courts have disagreed, finding that a plaintiff's diminished ability to sell his or her browsing data constitutes economic injury under the UCL, at least when a market exists for the data. *E.g.*, *Brown v. Google LLC*, No. 4:20-CV-3664, 2023 WL 5029899, at *21 (N.D. Cal. Aug. 7, 2023) (denying summary judgment on UCL claim where "Plaintiffs have shown that there is a market for their browsing data and Google's alleged surreptitious collection of the data inhibited plaintiffs' ability to participate in that market"). The discussion of standing in *Facebook Tracking*, on which Plaintiff relies, does not resolve this dispute, because that case did not address the UCL and considered only Article III standing. 956 F.3d at 597–601; *see Hazel v. Prudential Fin., Inc.*, No. 22-CV-07465, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) (rejecting reliance on *Facebook Tracking* to establish UCL standing because "as many courts have pointed out, a plaintiff may have Article III standing but nevertheless fail to demonstrate UCL standing").

On this record, it is not clear that Plaintiff has alleged economic injury sufficient to establish UCL standing. Plaintiff generally alleges that internet users' personal information and search data may be monetized, but she does not allege specific facts showing that she could have sold the limited data collected by the TikTok SDK through the three identified websites, that she has ever attempted or intended to sell her data, or that Defendants' collection of that data, without more, has impeded her ability to sell her data. *See Hazel*, 2023 WL 3933073, at *6 (dismissing UCL claim brought by plaintiffs whose data was intercepted without their knowledge or consent, since "just because Plaintiffs' data is valuable in the abstract, and because [defendant] might have made money from it, does not mean that Plaintiffs have 'lost money or property' as a result" (collecting cases)). Nor is Plaintiff a customer of Defendants who has received less than the benefit of her bargain based on the taking of her data. Indeed, a primary thrust of her complaint is that she has never interacted with Defendants.

In *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, Judge Chhabria found similar allegations insufficient to establish UCL standing:

> To have standing under California law to pursue this claim (a standard that is different from Article III standing), the plaintiffs must show that they "lost money or property" because of Facebook's conduct. [Citations omitted.] The plaintiffs' UCL claim fails because they have not adequately alleged lost money or property. As discussed in Section III, the plaintiffs' theory of economic loss is purely hypothetical.[6] It's true . . . that Facebook may have gained money through its sharing or use of the plaintiffs' information, but that's different from saying the plaintiffs lost money. Further, the plaintiffs here do not allege that they paid any premiums (or any money at all) to Facebook to potentially give rise to standing under California law.

402 F. Supp. 3d at 804. The Court finds this analysis, which appears consistent with the Ninth Circuit's decision affirming dismissal of the UCL claim in *In re Facebook Priv. Litig.*, 572 F. App'x 494, to be both persuasive and applicable to the allegations here. *See also Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 994 (2011) (affirming finding of no UCL standing where "[t]he fact that the [plaintiff's] address had value to Lamps Plus, such that the retailer paid Experian a license fee for its use, does not mean that its value to plaintiff was diminished in any way"). In the absence of allegations that Plaintiff incurred actual financial losses, for example because she wished to sell her browsing data but was unable to

---

[6] Section III of the analysis, referenced in the UCL standing analysis, addressed the plaintiff's lost value argument in the context of Article III standing:

> Regarding loss of value, although it's true that each user's information is worth a certain amount of money to Facebook and the companies Facebook gave it to, it does not follow that the same information, when not disclosed, has independent economic value to an individual user. The plaintiffs do not plausibly allege that they intended to sell their non-disclosed personal information to someone else. Nor, in any event, do they plausibly allege that someone else would have bought it as a stand-alone product. The plaintiffs' economic-loss theory is therefore purely hypothetical and does not give rise to standing.

In re Facebook, 402 F. Supp. 3d at 784.

do so or would be paid less for the data, she has not plausibly alleged economic injury for purposes of UCL standing. Count 5 is therefore dismissed.[7]

IV.

In her opposition, Plaintiff requests leave to amend if the Court determines that the motion should be granted. Dkt. No. 35 at 22. "The court should freely grant leave [to amend] when justice so requires," Fed. R. Civ. P. 15(a)(2), and the policy favoring amendments "is to be applied with extreme liberality," *Morongo Band of Mission Indians v. Rose*, 893 F.2d 1074, 1079 (9th Cir. 1990). This case is still at an early stage, Plaintiff has not previously amended her pleadings, and Defendants have neither opposed amendment nor shown that amendment would necessarily be futile. Accordingly, Plaintiff is granted leave to file a First Amended Complaint (FAC) by October 20, 2023.

V.

Defendants' motion to dismiss Plaintiff's complaint is GRANTED IN PART, and Plaintiff's claims in Counts 2 and 5 for violations of the CFAA and the UCL are DISMISSED. The motion is otherwise DENIED. Plaintiff may file her FAC no later than October 20, 2023. If she does not reallege the dismissed claims within the time allowed, their dismissal will automatically convert to a dismissal with prejudice (only as to Plaintiff individually).

Date: October 6, 2023

Stanley Blumenfeld, Jr.
United States District Judge

[7] Although Defendants' argument that Plaintiff's larceny and conversion claims should be dismissed because she lacks a property interest in her browsing information overlaps with their argument for dismissal of her UCL claim, the different claims raise distinct issues as framed and argued by the parties. The Court understands the parties to be raising arguments that distinguish between the existence of a property interest sufficient to support larceny and conversion claims, on the one hand, and the existence of economic loss associated with the alleged property interest sufficient to support a UCL claim, on the other. The Court's conclusion is that Plaintiff has plausibly alleged the former but not the latter.